Procedure Title: HIPAA Incident Response and Reporting **Number:** TD-QMP-P-7009	
Subject: Incident Reporting and Response Procedures	
Primary Department: TennDent/Quality Monitoring/Improvement	**Secondary Department:**
Effective Date of Procedure: 9/23/2011	**Prior Procedure or Cross Reference(s):** 10/1/2010
Last Reviewed by TennDent Quality Monitoring/Improvement Committee: 9/23/2011	**Date Procedure Last Revised:** 9/23/2011
Review Frequency: Annually	**Next Scheduled Review:** 7/1/2012
TennDent Quality Monitoring/Improvement Committee Approval: On File	**Approval Date:** 9/23/2011

Scope:

TennDent staff, network providers, and TennCare enrollees

Purpose:

TennDent is committed to conducting business in compliance with all applicable laws, regulations and TennDent policies. These procedures cover the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

Procedure:

Responsible Party	***Action***
All TennDent Staff	Users must notify Information Technology for issues involving viruses, local attacks, denial of service (DOS) attacks, etc. by completing a Security Incident Report Form. If an incident directly affects Electronic Personal Health Information (EPHI) the user must immediately notify his/her manager. If the manager is unavailable, the user should report the

	incident to the Information Security Officer.
TennDent Management Staff	Managers must notify Information Technology if the incident affects or may affect other systems and networks. Managers must notify their Information Security Officer if the incident is a threat to EPHI. If the Information Security Officer is unavailable, the HIPAA Privacy Officer should be notified.
TennDent IT Staff	Information Technology should investigate and propagate recommended updates or fixes to threatened or actual security incidents and complete the Security Incident Report Investigation Form. Information Technology also should notify the Information Security Officer if a threat to EPHI exists.
TennDent Management Staff	Each manager should aggregate and determine the severity of security incidents within their Department involving EPHI and report those incidents, when appropriate, to the Information Security Officer. Incidents that should be reported include, but are not limited to: a. Virus, worm, or other malicious code attacks b. Network or system intrusions c. Persistent intrusion attempts from a particular entity d. Unauthorized access to EPHI, an EPHI based system, or an EPHI based network e. EPHI data loss due to disaster, failure, error
HIPAA Security Officer HIPAA Privacy Officer	The HIPAA Security and Privacy Officers must notify each other of security or privacy issues if they determine that an incident or issue could affect the other office. The Information Security Officer must notify Information Technology if a security incident involves an outside entity or traverses TennDent backbone network.
HIPAA Privacy Officer	All correspondence with outside authorities such as local police, FBI, media, etc. must go through the CEO of TennDent.
HIPAA Security Officer	The Information Security Officer will document and log incidents and outcomes related to HIPAA Security.
HIPAA Security Officer	The Information Security Officer will notify the Officers/Managers of viruses and other malicious software and TennDent-wide threats to EPHI.

	Such notifications may be made by way of TennDent Email to distribution list of Officers and Managers.
TennDent Management Staff	The Officer/Manager is responsible for propagating these notifications within his/her TennDent Department and ensuring that appropriate measures are implemented to mitigate the harmful effects of such security threats based on such notifications.

Related Policies and Procedures:

HIPAA Data Backup and Contingency Planning Policy
HIPAA Data Backup Procedures
HIPAA Incident Reporting and Response Policy

Related Documents:

Security Incident Report Form
Security Incident Report Investigation Form

Security Incident Report Form

TD-QMP-F-7008

The purpose of this form is to report the facts pertaining to any known or suspected violation of TennDent's security standards or the laws and regulations governing TennDent. Although we ask you to provide your name, it is not necessary for you to do so if you wish to make an anonymous report. An anonymous report can be made by completing this form and mailing it to the Security Officer at TennDent. If you do not want to give your name, you may call the Security Officer within one week of submitting this report to inquire about the outcome of the investigation.

If you wish to identify yourself in this report, TennDent will make every effort to keep your identity confidential, unless you give TennDent permission to reveal it. Only the Security Officer, and others designated by the Security Officer, will have access to your report. No disciplinary action or retaliation will be taken against you for making a good faith report of a compliance violation.

Please include all the factual details of the suspected violation, however big or small, to ensure that the Security Officer has all of the information necessary to conduct a thorough investigation.

Please attach additional pages as needed. The information that you provide should include names, dates, times, places and a detailed description of the incident that led you to believe that a violation of TennDent's security standards occurred. Please include a copy or a description of any documents that support your concerns.

Date of this report: ____

Name of person making this report (optional): ____

Description of the violation(s): ____

Detailed description of the incident(s) resulting in the violation (include names, dates, times and places):

____

____

____

Name(s) of person(s) involved in the incident and an explanation of their role:

____

Name(s) of other person(s) having knowledge of the incident: ______________________________

____

Department where the incident occurred: ____

____

Date(s) of the incident: ____

Explanation of how you became aware of the suspected violation: _______________________________

____

Please attach or describe any documents that support your concern (include a description of the documents, the identity of the persons who wrote the documents, the dates of the documents, and the location of the documents).

____

____

____

____

____

____

____

____

____

____

Security Incident Report Investigation Form

TD-QMP-F-7009

Date of reported concern: ____

Name of person who received the report: ____

Name of person who made the report (state "unknown" if the report was made anonymously):

____

Date(s) of investigation: ____

Name(s) of person(s) investigating: ____

____

Name(s) of person(s) interviewed: ____

____

Description of documents reviewed: ____

____

____

Findings: ____

____

____

____

Plan of correction: ____

____

____

____

_________________________________ _________________________

Signature of Security Officer Date